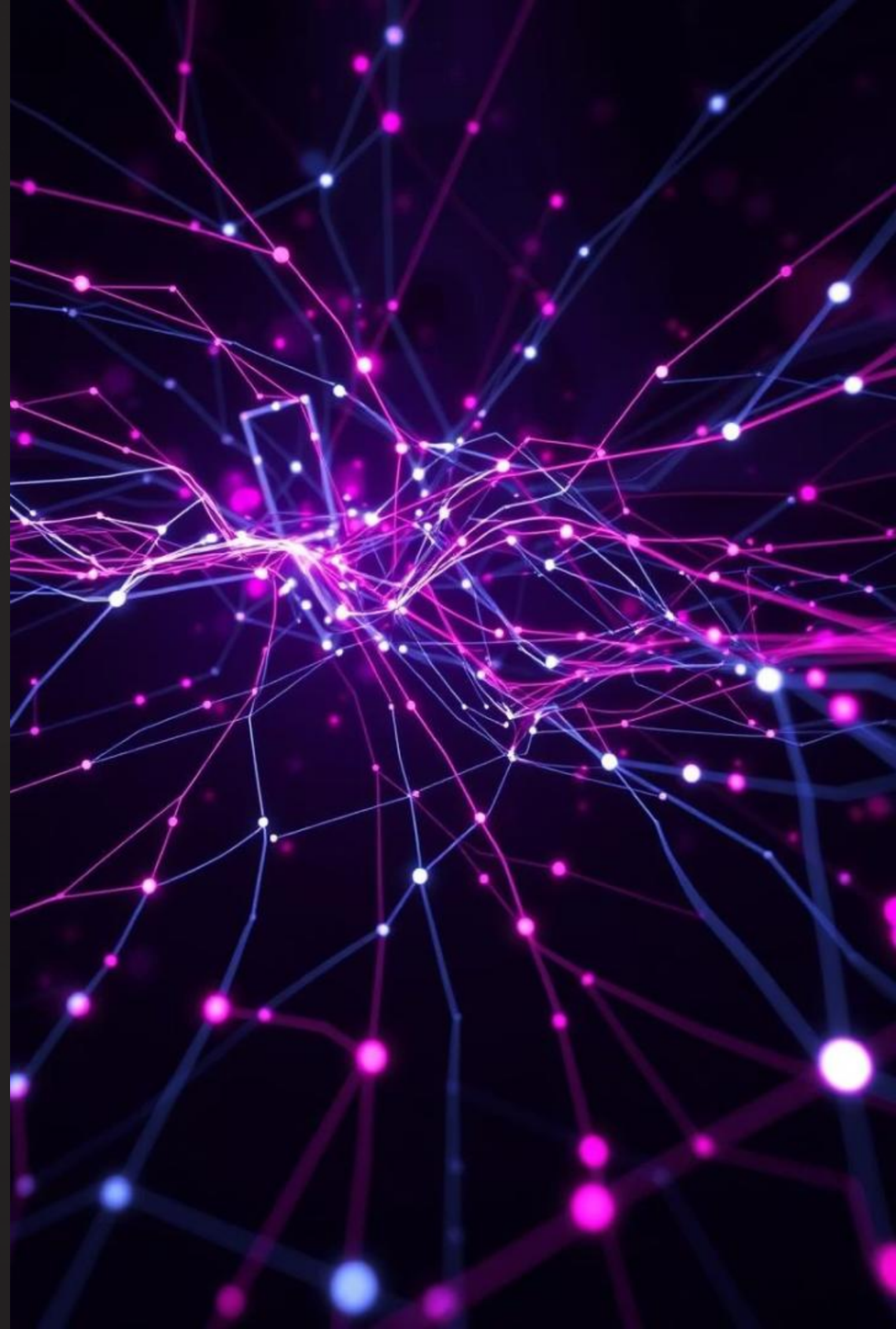
ILIDViz: Un sistema de análisis visual basado en aprendizaje incremental para la detección de anomalías en la red



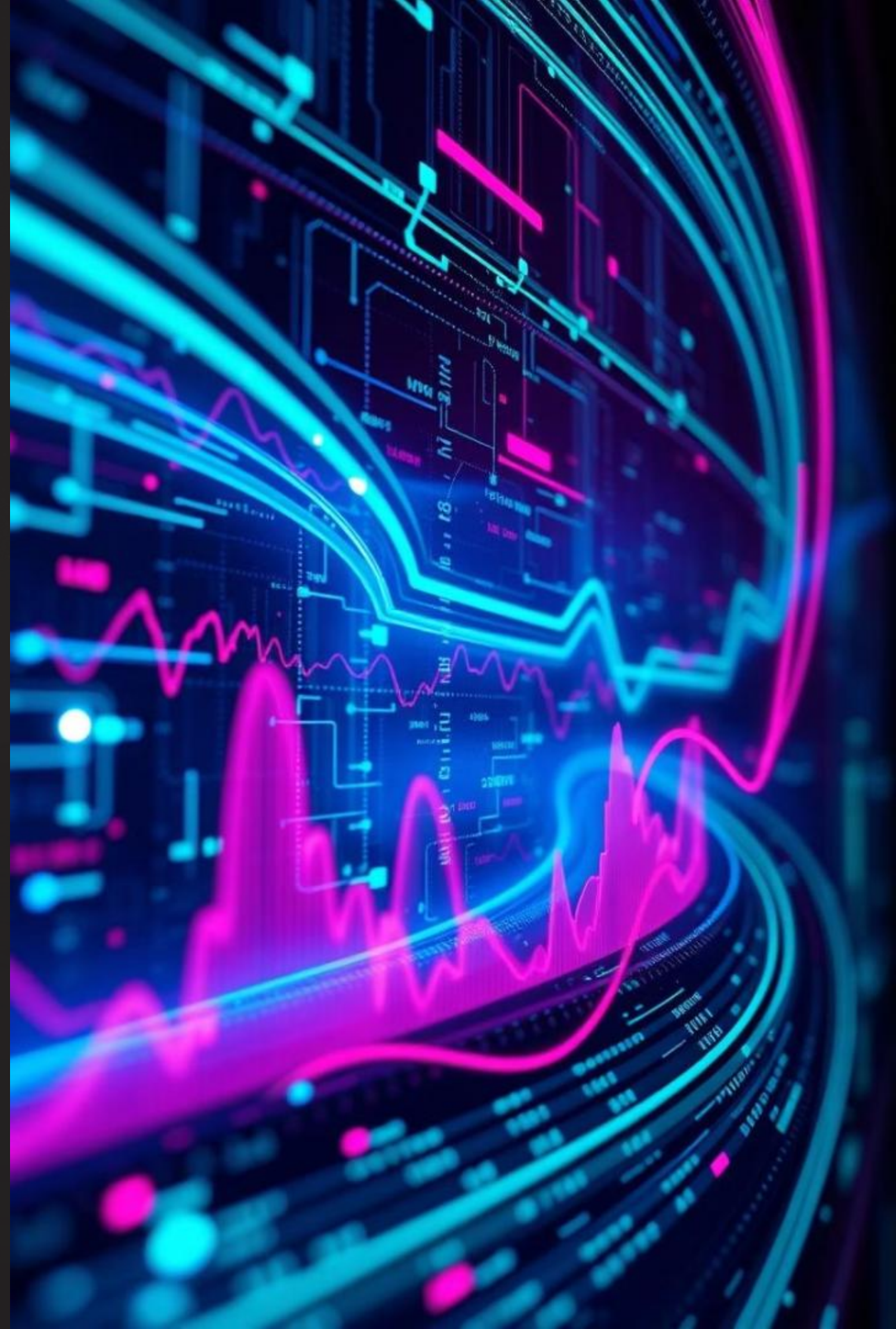
Problema

Los sistemas IDS actuales no detectan bien ataques desconocidos, no se adaptan en tiempo real y dependen de datos etiquetados.

Objetivo del artículo

Desarrollar un sistema que aprenda de forma incremental, seleccione qué datos etiquetar y brinde apoyo visual al analista.

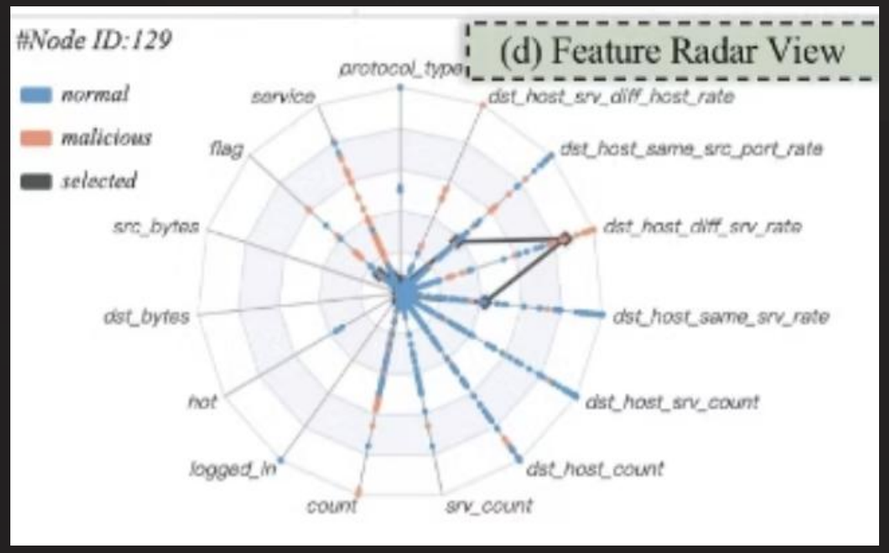
Meta: extenderlo a un **sistema en tiempo real funcional y continuo**.



Propuesta: ILIDViz

ILIDViz combina aprendizaje activo con visualización interactiva y el algoritmo KAN-SOINN para análisis adaptativo de intrusiones.

Permite comparar visualmente un nodo seleccionado con patrones normales y maliciosos, ayudando al analista a identificar anomalías en múltiples atributos simultáneamente. Cada eje representa una característica del tráfico, y los colores (azul, rojo, negro) diferencian entre clases y el nodo bajo análisis.



UNSA
UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

Conclusión

Aunque ILIDViz mejora la detección incremental, aún no opera en tiempo real, lo cual es el siguiente gran desafío para su implementación práctica.

Mejora la detección incremental

No opera en tiempo real

Próximo desafío: implementación práctica

UNSA

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

FSA-IDS: A Flow-based Self-Active Intrusion Detection

Problema

Los sistemas IDS basados en aprendizaje automático dependen fuertemente de datos etiquetados, los cuales son escasos, costosos y difíciles de obtener.

Objetivo

Reducir la necesidad de intervención humana mediante un sistema que aprenda de manera más eficiente usando aprendizaje activo.

UNSA

UNIVERSIDAD NACIONAL DE SAN AGUSTÍN DE AREQUIPA

Propuesta

FSA-IDS combina aprendizaje activo con agrupamiento (cluster-based sampling) para priorizar qué muestras etiquetar y mejorar la detección.

conclusión: El sistema mejora la detección y reduce el esfuerzo humano hasta en un 47%, usando datasets reales de tráfico benigno y malicioso.

Limitación clave: FSA-IDS no opera en tiempo real ni ha sido probado sobre tráfico en vivo, lo que limita su uso en entornos críticos con amenazas en curso.

47%

Reducción del esfuerzo humano

Gracias al aprendizaje activo y el agrupamiento.

Visual Analytics para la Detección Temprana de Intrusiones en Tiempo Real

Problema
Los sistemas IDS actuales no permiten visualizar ni adaptarse efectivamente a nuevos patrones de tráfico malicioso **en tiempo real**, lo que limita la reacción ante amenazas emergentes.

Objetivo
Diseñar una solución de análisis visual que permita detectar y visualizar **en tiempo real** patrones maliciosos desconocidos, ayudando a la intervención del analista.

Propuesta
Una herramienta visual que combine:
•Visualización interactiva del tráfico.
•Identificación de flujos sospechosos en tiempo real.
•Criterios de incertidumbre para apoyar decisiones humanas.

El **CICIDS2017** (Canadian Institute for Cybersecurity Intrusion Detection System 2017) es un conjunto de datos de referencia ampliamente utilizado en la investigación de ciberseguridad para evaluar modelos de detección de intrusiones.

•Fue creado por el **Canadian Institute for Cybersecurity** (CIC), en la **University of New Brunswick (Canadá)**.

•Contiene tráfico real y simulado generado en un entorno de red realista con distintos perfiles de ataque y usuarios normales.

Características destacadas

•Más de **80 atributos** por flujo (como duración, tamaño de paquetes, tiempo entre paquetes, etc.).

•**Etiquetas** detalladas: cada fila indica si el tráfico es normal o malicioso, y qué tipo de ataque es.

•Tráfico separado por días, con ataques específicos por día (por ejemplo: viernes DDoS).

Cosas a tener en cuenta

•Está **ligeramente desbalanceado**: hay más tráfico benigno que malicioso en algunos días.

•Algunos atributos pueden tener muchos valores nulos o ser irrelevantes (se recomienda limpieza previa).

•No es en tiempo real, pero puede usarse para **simular entornos real-time** al procesarlo por flujo o ventana temporal.

Columna	Tipo de dato	Descripción
Flow ID	object	Identificador único del flujo generado a partir de IPs, puertos y protocolo.
Source IP	object	Dirección IP del host que inicia el flujo de red.
Source Port	int64	Puerto utilizado por el emisor para la conexión.
Destination IP	object	Dirección IP del equipo receptor del flujo.
Destination Port	int64	Puerto al que se dirige el tráfico (p. ej., 80 para HTTP).
Protocol	int64	Protocolo de red utilizado (6: TCP, 17: UDP, 1: ICMP).
Timestamp	object	Hora exacta en la que comenzó el flujo.
Flow Duration	int64	Duración del flujo de red en milisegundos.
Total Fwd Packets	int64	Número total de paquetes enviados desde el emisor.
Total Backward Packets	int64	Número total de paquetes recibidos en respuesta.
Total Length of Fwd Packets	int64	Tamaño total de todos los paquetes enviados (bytes).
Total Length of Bwd Packets	int64	Tamaño total de todos los paquetes recibidos (bytes).
Fwd Packet Length Max	int64	Tamaño máximo de un paquete enviado.
Fwd Packet Length Min	int64	Tamaño mínimo de un paquete enviado.
Fwd Packet Length Mean	float64	Promedio del tamaño de los paquetes enviados.
Fwd Packet Length Std	float64	Desviación estándar del tamaño de paquetes enviados.
Bwd Packet Length Max	int64	Tamaño máximo de paquete recibido.
Bwd Packet Length Min	int64	Tamaño mínimo de paquete recibido.
Bwd Packet Length Mean	float64	Promedio del tamaño de los paquetes recibidos.
Bwd Packet Length Std	float64	Desviación estándar del tamaño de paquetes recibidos.
Flow Bytes/s	float64	Promedio de bytes transmitidos por segundo en el flujo.
Flow Packets/s	float64	Promedio de paquetes transmitidos por segundo.